# Darktrace announces acquisition of Cado Security to enhance cloud forensics capabilities



Darktrace, a leader in artificial intelligence-driven cybersecurity solutions, has announced plans to acquire Cado Security, a company based in the UK that specializes in cyber investigation and response. The acquisition is expected to be completed by February 2025, subject to regulatory approval, and forms part of Darktrace’s strategy to enhance its capabilities in cloud forensics.

This strategic move is set to combine Cado Security’s advanced forensic investigation technologies with Darktrace’s existing ActiveAI Security Platform. According to the company, this integration will improve the efficiency of its Cyber AI Analyst, streamlining the processes of collecting and analysing data from various cloud environments. The enhancement aims to provide more robust support to cybersecurity teams as they face increasing threats in cloud-based infrastructures.

The acquisition not only strengthens Darktrace’s position in the market but is also driven by the impressive credentials of Cado Security’s founding team. James Campbell, the co-founder and CEO of Cado Security, has held significant roles in cybersecurity, having previously worked at PwC and as the Assistant Director of Operations for Australia’s National Incident Response capability at the Australian Signals Directorate. Chris Doman, the co-founder and Chief Technology Officer, is recognised for his contributions to the development of the ThreatCrowd threat intelligence platform, which was integral to the AlienVault Open Threat Exchange before its acquisition by AT&T.

Darktrace's intentions in cloud security have been further underscored by recent product deployments such as Darktrace/CLOUD for AWS and Microsoft Azure, indicating a strong focus on combatting the growing concerns related to cloud-based cyber threats. Research suggests that platforms operating in the cloud and Software as a Service (SaaS) applications remain prime targets for cyberattacks, making this acquisition particularly timely.

Furthermore, the collaboration between Cado Security’s research and development teams, located in London and Bristol, and Darktrace’s R&D centres in Cambridge, UK, and The Hague, Netherlands, is aimed at accelerating innovation in cloud detection and response solutions. This move reflects Darktrace's broader commitment to developing technology that can respond to the shifting paradigms of cybersecurity threats in a cloud-dominant environment.

Jill Popelka, the CEO of Darktrace, has emphasised the significance of Cado’s expertise in cloud forensics in facilitating improved client protections through enhanced data collection and investigation tools. Additionally, James Campbell shared his enthusiasm regarding the partnership, highlighting how the strengths of both companies align with their goals of continuous innovation and growth.

The acquisition follows Darktrace’s recent buyout by private equity firm Thoma Bravo, marking an ongoing strategic endeavour to expand its portfolio of AI-augmented cybersecurity solutions. By bolstering its capabilities in cloud forensics and incident response, Darktrace aims to effectively tackle the evolving cybersecurity challenges posed by an increasingly cloud-centric digital landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Corroborates Darktrace's plans to acquire Cado Security, the expected completion date, and the integration of Cado's technologies with Darktrace's ActiveAI Security Platform.
2. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Provides details on Cado Security’s expertise in cloud data forensics and automation, and how it will enhance Darktrace’s cybersecurity capabilities.
3. <https://darktrace.com/news/darktrace-transforms-security-operations-and-improves-cyber-resilience-with-launch-of-darktrace-activeai-security-platform> - Explains the features and capabilities of Darktrace’s ActiveAI Security Platform, including its ability to visualize, correlate, and investigate security incidents across various domains.
4. <https://industrialcyber.co/news/darktrace-introduces-activeai-security-platform-to-boost-security-operations-cyber-resilience/> - Further details on the ActiveAI Security Platform’s core detection and autonomous response capabilities, and its role in transforming security operations.
5. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Mentions the credentials of Cado Security’s founding team, including James Campbell and Chris Doman, and their significant roles in cybersecurity.
6. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Highlights Darktrace’s recent product deployments such as Darktrace/CLOUD for AWS and Microsoft Azure, indicating a strong focus on cloud security.
7. <https://darktrace.com/news/darktrace-transforms-security-operations-and-improves-cyber-resilience-with-launch-of-darktrace-activeai-security-platform> - Supports the integration of Cado Security’s R&D teams with Darktrace’s R&D centres to accelerate innovation in cloud detection and response solutions.
8. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Quotes Jill Popelka, the CEO of Darktrace, on the significance of Cado’s expertise in cloud forensics and its impact on client protections.
9. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Mentions James Campbell’s enthusiasm regarding the partnership and the alignment of both companies’ goals for continuous innovation and growth.
10. <https://sitsi.pacanalyst.com/darktrace-intends-to-acquire-cado-security/> - Notes the acquisition follows Darktrace’s recent buyout by private equity firm Thoma Bravo, as part of an ongoing strategic endeavour to expand its AI-augmented cybersecurity solutions.
11. <https://cisotimes.com/darktrace-to-acquire-cado-security-strengthening-cloud-forensics-and-cybersecurity-capabilities/> - Please view link - unable to able to access data